DATA PROTECTION
POLICY AND PROCEDURES

LOCATION	SHAREPOINT > STAFF > DOCUMENTS > GENERAL > POLICIES AND PROCEDURES> POLICIES		
LAST APPROVED	SEPTEMBER 2023	REVIEW CYCLE	JULY/SEPTEMBER
TO BE REVIEWED ANNUALLY			

RELATED POLICIES AND PROCEDURES	
Privacy notice	Acceptable IT Equipment Use Policy
Personnel policy	Confidentiality policy and declaration

CONTEXT AND OVERVIEW

CHAT needs to gather and use certain personal information about individuals. This can include clients, staff, volunteers, trustees, donors, and members.

All data must be collected, stored and managed in accordance with UK law, and in line with our ethos and values. Individuals retain the rights over their own data at all times. Our use of their data must be fair and lawful, and we must be open and honest about what we do with people's data.

All data we process is in accordance with the rules as laid down in statute, including the General Data Protection Regulations and the Data Protection Act 2018.

This policy applies to:

- All sites within our organisation
- Our staff, volunteers and trustees, contractors, suppliers and anyone working on our behalf

Key principles

The UK GDPR sets out seven key principles:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

These principles lie at the heart of our approach to processing personal data.

This policy will help ensure that CHAT respects the rights of all individuals whose data it collects. It encompasses legal responsibilities and best practice. By being open and honest with individuals we will demonstrate that people can trust our organisation and that we handle personal data with integrity. Routine application of these principles will also help protect CHAT from the risk of data breaches and unauthorised access to personal information.

Data Protection Law and Principles
The use of personal data is governed by UK law. This is enhanced and explained by case law and best practice.

In order to comply with the law, personal data must be collected fairly and lawfully. It must be stored safely and managed securely. It must not be disclosed to anyone who does not have authority to see it.

The General Data Protection Regulations (GDPR) set out how data should be obtained, stored and handled. These regulations set out seven principles that underpin lawful use of data. These provide the foundation for good data governance. These principles are enhanced by a range of powers for individuals to control how their data is processed and stored.

Responsibilities under this policy
Everyone who works with or for CHAT has some responsibility for ensuring that data is handled safely, securely and appropriately.

There are key roles within the organisation that carry specific responsibilities.

The **Board of Trustees** are the strategic lead body for the organisation. They will bear ultimate responsibility for ensuring that all our legal obligations are met. They will be accountable for any failure to abide by the correct regulations and for any impact that they may have on our clients and our reputation within the local area. The Board of Trustees' lead on Data Protection is Rod Hewson.

The Manager is the operational lead for the organisation. They must ensure that all relevant policies and procedures are in place, and that practice follows the policy across all areas of work. They will liaise with the Data Protection Lead in the event of any data governance issues that require attention and will have overall responsibility for setting an appropriate tone of respect for personal data within CHAT.

The Manager is responsible for liaising with IT suppliers to ensure the physical and virtual integrity of IT data storage services, systems and equipment. They will ensure all IT security meets acceptable professional standards, appropriate to the needs of the organisation, and that access to all electronic systems, databases or files is managed in accordance with the relevant polices. They will liaise with any 3rd party used for processing data, such as an HR / payroll supplier or cloud computing provider, to ensure appropriate levels of protection for all personal data. They have responsibility for making sure that client-facing applications such as websites or online forms comply with relevant regulations including cookie policies and privacy notices. They will also oversee the life-cycle of data, software and hardware, ensuring that the processes for deleting or encrypting files function effectively.

The Data Protection Lead has a key role to play in providing expert advice and guidance to the Board of Trustees and the Manager. It is their responsibility to update the Manager and the Board of Trustees about Data Protection issues, and give advice regarding policies and procedures following legislative and best practice updates. They will oversee training and guidance for all staff (employees and volunteers), and along with the Manager be responsible for liaison with 3rd party suppliers, contractors and partners if they handle personal data. The Manager and Data Protection Lead will also oversee any Subject Access Requests, and handle the response to any data breaches, including being the point of contact for the public and notifying the ICO where

necessary. **The Data Protection Lead is currently Denise Henson who works closely with the Manager.**

What is personal data?
Personal data is information about a person - anything that would allow someone to identify a living individual. Processing that data means obtaining, using, and transferring data, and storing it in any system that allows it to be found again, such as a computer database or filing system.

Our Privacy Notice
CHAT will take all reasonable steps to ensure that individuals are aware their data is being processed. This will include telling individuals what is being used, how it is being used, how long it will be kept for, and how they can exercise their rights in respect of that data.

Our Privacy Notice sets out how we collect data, what data we collect, the lawful basis for that, and how long we retain it. It includes information on who we share data with and the lawful basis for such sharing. It also sets out how people can request copies of data we hold about them. The Notice will be freely available on request, and on the organisation's website.

Keeping personal data secure
Once personal data has been lawfully and fairly collected and processed, it must be safely stored, kept up to date, and safely accessed. Storing data in a way that complies with the regulations is a mix of common sense, clear processes and application of strong IT solutions.

The only people who will have access to personal data at CHAT are those who need it for their work. Our IT systems and file storage will have granular levels of permission, and we will ensure that people only see personal data if required for operational reasons and to deliver our services professionally.

Strong passwords must be used to access electronic resources and IT systems. These should never be shared with other people or written down. Computer and database passwords must be changed on a 6-monthly basis.

Personal data must only be disclosed to those who are authorised to see it, both within and outside the organisation. If there is any doubt about the identity of the person requesting access to information, or doubt as to whether they should be allowed to see it, do not disclose information.

Data will only be shared with those people who are authorised to see it. This will be in line with our legal obligations and with the lawful and legitimate requirements of the business. Our Privacy Notice explains who we might share data with, the lawful basis for that, and the circumstances in which you can object to data being shared.

An appropriate level of training for all staff and trustees will be given. This will help them understand their responsibilities under data protection legislation. Staff should ask the Manager or the Data Protection Lead for guidance if they are unsure about any aspect of data protection.

Data use and transfer
Data must only be used for the purpose it was first obtained. Personal data should not be shared informally, either internally or externally to the organisation.

Staff should follow simple checks when transferring data outside the organisation via post or email, to ensure that personal data goes to the correct recipient. We will use a simple checklist when sending personal data by post, to add an extra layer of security and checking to our data transfers. Extra care must be taken when sharing data via email. This might include encryption or use of a secure email client.

Data should never be stored on personal IT devices. In particular staff must not email CHAT documents to their personal email addresses. If data needs to be transferred outside of the organisation staff should use their CHAT email account or *a* secure cloud storage solution provided by the Manager

Marketing and Promotion
We will ensure that anyone receiving marketing or promotion communications from us has given positive consent to receiving those communications, in the format that we send them out.

CCTV
CHAT uses CCTV cameras on our site at Coggan's Well House. This is to ensure the safety and security of those in our community, and to protect the site from damage. Our use of CCTV follows best practice guidelines as laid down by the Information Commissioner's Office (ICO).

Images recorded by the CCTV cameras are stored in a secure location. They are retained for a maximum of 30 days after which time they are securely overwritten.

Access to the images is restricted to specified people within CHAT We will only view CCTV footage in response to an incident or an allegation. The images on our CCTV system are of a sufficient quality to allow us to make out faces of individuals in most circumstances. We are able to take copies of relevant parts of the CCTV footage and store it securely, in order to assist investigations into incidents or allegations.

In certain circumstances we may share CCTV footage with partners or other agencies. This may include the Local Authority or the Police. Anyone can ask to see CCTV footage in which their image is captured and this should be done in writing as part of a Subject Access Request.

Getting consent to process personal data
There may be times where we would like to process data in a way that requires an individual's consent. This could include taking photographs or images of individuals engaging in our activities, or adding contact details to any marketing or promotional mailing lists

CHAT will ensure that we obtain consent in a positive and clear way and individuals will be able to refuse consent. We will also ensure that consent can be withdrawn quickly and easily.

Subject Access Requests
Anyone has the right to ask to see a copy of any information we hold about them. This is known as a Subject Access Request (SAR) and can be done verbally, by writing to us at Churches Housing Action Team (Mid Devon) Ltd., Coggan's Well House, Phoenix Lane, Tiverton, EX16 6LU or email us at theoffice@chatmid.co.uk. All SARs will be referred to the Data Protection Lead or the Manager.

PROCEDURE

- The Privacy Notice is explained when we first meet with new clients and they are offered a copy.
- All new clients will have explained to them the client agreement and the advisor will ensure that they understand how we process their data and providing their consent including how they prefer to be contacted
- If any client data or equipment that has data on it is lost this will be reported to the manager or data protection lead without delay
- Equipment or any documents containing client data will not be left unattended in the public area of CHAT
- Emails containing client data will be uploaded to Advice Pro and then deleted
- Care must be taken when sending post. All outgoing letters must be checked to ensure nothing extra is in the envelope and the booked signed. A return address should be on the envelope.
- All documents should be collected from printers as soon as possible to avoid confusion of confidential information.
- Passwords must not be shared ever.
- Desks must be clear at the end of the day with all information locked away.
- All files should be stored on the 'shared' area and not on the desktop of any computer. Once they have been uploaded to Advice Pro or stored on the client file they can be deleted
- Laptops and mobiles must be locked away when not in use.
- Files and equipment must be signed out and back in.
- Confidentiality agreements will be signed by anyone who has access to client data.
- Data Protection will be discussed at staff and trustee meetings and training done as part of the induction process with regular refreshers.
- All our marketing and promotion communications will include a simple process for opting out of future communications.
- Email and phone use is monitored as outlined in our acceptable use policy.
- Laptops, files and any confidential information must be locked away while working elsewhere (from home for example)

FILE DESTRUCTION POLICY

The Personnel data policy and employee handbook give more information about retention periods in relation to all staff. These records are kept by the Manager who is also responsible for identifying the records and destroying all records after the period specified.

Case records are stored securely for a minimum of six years from the last date of contact, or twelve years if the case involved mortgage advice before they are destroyed.

FILE DESTRUCTION PROCEDURE

- When files are destroyed care will be taken that all paper files together with associated documents and correspondence are shredded (in-house or with a reputable firm) and the electronic data is permanently deleted from the database along with all associated computer files.

- The Manager is responsible for delegating the task of identifying and removing old files periodically and cases on Advice Pro will be automatically archived (with only anonymised data kept on the system). This will be carried out at least every three months.